La Protection des Données Personnelles

Bénédicte Deleporte
Avocat

Protection des Données Personnelles

- Objectifs du cours:

  - Etudier les principes généraux applicables au domaine de la protection des données personnelles en France et dans l'UE

  - Les règles spécifiques applicables à la protection des données personnelles et internet

  - Les principes applicables aux transferts de données internationaux

Protection des Données Personnelles

- **Thèmes couverts:**

- **Introduction: Comment est réglementé le domaine de la protection des données?**

- **Etendue de la protection des données**
- **La Commission Nationale de l'Informatique et des Libertés (CNIL)**
- **Les principes applicables à la collecte de données à caractère personnel**
- **Les principes applicables à la protection des personnes et à leurs données**
- **Les obligations applicables au responsable du traitement de données**

- **La protection des données et internet**

- **Les transferts de données à l'international**

Protection des Données Personnelles

- **Introduction - Comment est réglementé le domaine de la protection des données?**
  - **La France a été l'un des premiers pays à mettre en oeuvre une législation sur la protection de la vie privée avec la Loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 (Loi Informatique et Libertés).**
    - **Basé sur les droits fondamentaux relatifs à la protection des droits de l'Homme**
    - **En réaction au développement de l'informatique dans la société et des bases de données automatisées**

  - **L'Union européenne a publié la Directive sur la protection des données le 24 octobre 1995**
    - **La France a été le dernier pays-membre de l'UE à transposer la directive (et à modifier la loi de 1978) le 8 août 2004!**
    - **Transposition plus rapide dans les pays qui n'avaient pas de loi sur la protection de la vie privée**

Protection des Données Personnelles

- **Introduction - Comment est réglementé le domaine de la protection des données?**
  - Projet de règlement européen sur la protection des données personnelles devrait être adopté avant la fin de 2014
  - Sera applicable directement dans tous les états-membres de l'Union
  - Grands principes seront les mêmes qu'actuellement
  - Des changements concernant notamment les règles de déclaration des traitements de données et les attributions des commissions nationales (CNILs)
  - Remplacera la loi Informatique et Libertés

Protection des Données Personnelles

- **Etendue de la protection des données**

  • En vertu de l'article 2 al.2 de la Loi Informatique et Libertés du 6 janvier 1978, le domaine de la protection des données s'applique aux <u>données à caractère personnel</u>, à savoir:

  - "toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres"

  - tels que nom, numéro d'identification, voix, image, empreintes génétiques, adresse IP, numéro de téléphone, etc.

Protection des Données Personnelles

- **Etendue de la protection des données**

  - **Application à tous types de données personnelles, qu'elles fassent l'objet d'un traitement automatisé ou manuel**

  - **Tous les types de traitements suivants sont soumis à la loi de 1978:**
    - La collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la diffusion, la comparaison, l'interconnexion, la suppression, etc. des données à caractère personnel

  - **Les seuls traitements de données non couverts par la réglementation sont ceux mis en oeuvre exclusivement pour une finalité personnelle**

Protection des Données Personnelles

- La Commission Nationale de l'Informatique et des Libertés (CNIL) - son rôle et ses pouvoirs

  - La loi Informatique et Libertés de 1978 a prévu la création de la Commission Nationale de l'Informatique et des Libertés (CNIL)

    - La CNIL a la charge de:
      - assurer l'application et le respect de la loi Informatique et Libertés
      - émettre des avis, délibérations et recommandations sur la base des questions et problèmes pratiques soulevés par le développement de nouveaux types de traitements de données. Ces documents sont utilisés pour aider à interpréter et compléter la réglementation.

Protection des Données Personnelles

- La Commission Nationale de l'Informatique et des Libertés (CNIL) - son rôle et ses pouvoirs

  ▸ Avec la transposition de la directive de 1995, la CNIL a vu ses pouvoirs de contrôle a posteriori renforcés: La Commission peut décider, de sa propre initiative, de <u>contrôler</u> le respect par toute personne morale des traitements de données mis en oeuvre au regard de la réglementation

  ➡ Peut avoir accès aux locaux professionnels

  ➡ y compris aux matériels utilisés pour les traitements de données et à tous documents

Protection des Données Personnelles

- Principes applicables à la collecte de données personnelles

  • Deux principes de base s'appliquent à toute collecte de données à caractère personnel:

  - Principe de loyauté
  - Principe de proportionnalité

Protection des Données Personnelles

- **Principes applicables à la collecte de données personnelles**

  - Le principe de <u>loyauté</u>: Les collectes et traitements de données doivent être effectués de manière loyale et licite pour des finalités déterminées, explicites et légitimes (art. 6 de la loi Informatique et Libertés)

- Seules les données objectives strictement liées à la finalité du traitement peuvent être collectées légalement.

- La collecte et le traitement des données sensibles sont strictement réglementés

  - Les données sensibles sont les données concernant les origines raciales ou ethniques; les opinions politiques, philosophiques ou religieuses; l'appartenance à un syndicat; l'orientation sexuelle.

Protection des Données Personnelles

- **Principes applicables à la collecte de données personnelles**

  • Le principe de <u>proportionnalité</u>: La collecte de données doit être loyale et en adéquation avec la finalité du traitement.

  - Les données doivent être adéquates, correctes, complètes, pertinentes, et non excessives par rapport à la finalité pour laquelle elles sont collectées.

Protection des Données Personnelles

- **Principes applicables à la collecte de données personnelles**

  • Toute collecte de données illégale, déloyale ou frauduleuse et toute modification de la finalité du traitement de données est constitutive d'un manquement à la réglementation.

  - La personne responsable du manquement voit sa responsabilité civile engagée (Art 1382 du code civ.)
  - ainsi que sa responsabilité pénale, à savoir 5 ans d'emprisonnement et 300.000€ d'amende. (art. 226-18 du code pénal)

Protection des Données Personnelles

- **Principes applicables à la collecte de données personnelles**

  • Définition d'une collecte de données illicite donnée par la cour de cassation dans un arrêt du 3 novembre 1987: "Caractérise des moyens frauduleux, déloyaux ou illicites, la collecte de données auprès de tiers à l'insu des intéressés et sans déclaration de traitement."

  - Exemple de la page données personnelles des sites Amazon.fr et Priceminister.com:

    - http://www.amazon.fr/gp/help/customer/display.html?ie=UTF8&nodeId=3329781
    - http://www.priceminister.com/help/i_priv_cookies

Protection des Données Personnelles

- **Principes applicables à la protection des personnes et à leurs données personnelles**

  - L'accord <u>exprès</u> et <u>préalable</u> de la personne concernée par la collecte

    - Le responsable du traitement doit fournir les informations suivantes à la personne concernée préalablement à la collecte de ses données:

      - Identification du responsable du traitement; Objet du traitement; Existence d'un droit d'accès, de contestation, de correction ou d'opposition à la collecte; Le caractère obligatoire ou facultatif des réponses et les conséquences éventuelles d'un refus de répondre; Identification du destinataire des données collectées; Si les données sont transférées en dehors de l'UE.

Protection des Données Personnelles

- **Principes applicables à la protection des personnes et à leurs données personnelles**

  - **Il existe des exceptions au principe du consentement exprès et préalable, lorsque la collecte est faite avec les finalités suivantes:**
    - **Lorsque le responsable du traitement doit respecter une obligation légale (ex: immatriculation automobile et données figurant sur la carte grise)**
    - **Pour sauvegarder la vie de la personne concernée (entrée à l'hôpital)**
    - **Lorsque le responsable du traitement a une mission de service public (déclaration et paiement des impôts…)**
    - **Dans le cadre de l'exécution d'un contrat avec la personne concernée**
    - **Lorsque le responsable du traitement remplit un intérêt légitime (interprétation restrictive)**

Protection des Données Personnelles

- **Principes applicables à la protection des personnes et à leurs données personnelles**

  - Droit d'accès
    - La personne concernée a un droit d'accès à ses données personnelles aux fins suivantes:
      - Modification et mise à jour de ses données
      - Contestation du traitement de données
      - Opposition à la collecte de données (par rapport aux campagnes marketing et aux activités de prospection commerciale)

Protection des Données Personnelles

- **Obligations applicables à la personne physique ou morale traitant les données**

- **La personne qui collecte et traite les données personnelles doit respecter les obligations suivantes:**

  - **Obligation de déclarer le traitement de données**

  - **Obligation de sécurité**

  - **Auto-régulation et Codes de conduite**

Protection des Données Personnelles

- **Obligations applicables à la personne physique ou morale traitant les données**

- **Obligation de déclaration du traitement de données <u>préalablement à sa création</u>:**

  - **Deux systèmes sont applicables à tout nouveau traitement de données personnelles, compte tenu de la finalité du traitement et du type de données collectées:**

    - **La déclaration du traitement de données à la CNIL**

    ou

    - **La demande d'autorisation à la CNIL**

Protection des Données Personnelles

- Obligation de déclaration du traitement à la CNIL

  - Il existe deux systèmes de déclaration:

    - La déclaration "normale"

    - La déclaration "simplifiée"

Protection des Données Personnelles

- La déclaration "normale":

  - La loi prévoit une obligation de déclaration applicable à tout nouveau traitement de données (qu'il soit ou non informatisé) auprès de la CNIL

  - Exemples de traitements de données soumis à déclaration préalable:
    - Traitements dont la finalité est le contrôle de l'activité professionnelle des salariés (vidéosurveillance, utilisation de l'internet et de la messagerie, géolocalisation); Les traitements liés à l'embauche (bases de données de candidats, CV); Les fichiers médicaux informatisés; les fichiers utilisés par les comités d'entreprise; Les traitements transférés en dehors de l'Union européenne.

Protection des Données Personnelles

- La déclaration "normale":

  - Tout manquement à l'obligation de déclaration d'un traitement de données personnelles peut engager la responsabilité pénale et est passible d'une peine d'emprisonnement de 5 ans et/ou d'une amende de 300.000€

  - Les sites web exploités par des personnes physiques à des fins personnelles sont exemptés de l'obligation de déclaration des fichiers

Protection des Données Personnelles

- La déclaration "simplifiée":

  • La loi prévoit un système de déclaration simplifiée en ligne, pour la plupart des traitements de routine, lorsque leur mise en oeuvre ne porte pas atteinte à la vie privée ni aux droits fondamentaux des personnes.

  - Ces traitements de données doivent être conformes aux normes publiées par la CNIL

  - La CNIL a publié plusieurs normes simplifiées, par ex.:
    - La norme 72 sur le contrôle d'accès aux locaux professionnels et sur la gestion du temps de travail et des congés
    - La norme 46 sur les traitements les plus fréquemment mis en oeuvre par les services des ressources humaines (gestion du personnel, utilisation des matériels informatiques, organisation du travail, gestion de carrière, formation)
    - La norme 48 sur les fichiers clients et gestion des prospects

Protection des Données Personnelles

• Obligation de déclaration des traitements de données personnelles à la CNIL: Exemptions

• Suite à la transposition de la Directive en droit français, les entreprises peuvent désormais désigner un "correspondant informatique et libertés - CIL".

- Le CIL a la charge de s'assurer que tous les traitements mis en oeuvre par l'entreprise sont conformes à la loi et que le principe de respect de la vie privée est dûment appliqué au sein de l'entreprise.
- Sa mission inclus également l'obligation de conserver une liste à jour de tous les traitements internes, d'effectuer des formations en interne sur les questions liées à l'informatique et aux libertés et de mener des audits informatique et libertés réguliers.
- La nomination d'un CIL n'est pas obligatoire. Si un CIL est désigné par une société, sa désignation doit être déclarée et approuvée par la CNIL.
- L'entreprise reste responsable en cas de violations à la loi
- Le CIL peut être un tiers à la société (ex. consultant)

• Les entreprises disposant d'un CIL sont exemptées de l'obligation de déclaration pour la plupart des traitements de données

Protection des Données Personnelles

- Obligation de demander l'autorisation de la CNIL pour la mise en oeuvre de certains types de fichiers

  - Certains types de fichiers sont soumis à un contrôle renforcé de la part de la CNIL par le biais de son autorisation préalable
    - Soit à cause de la catégorie de données collectées (données sensibles)
    - Soit à cause de la finalité du traitement

  - Il existe 8 catégories de traitements à risque soumis à l'autorisation de la CNIL (art. 25 de la loi de 1978), notamment:
    - Les fichiers de statistiques (INSEE, etc.) qui contiennent des données relatives aux origines raciales ou ethniques, etc. sans l'accord exprès de la personne intéressée sont interdits. Les dérogations sont strictement réglementées.
    - Les traitements automatisés concernant les données génétiques, sauf pour les traitements mis en oeuvre par des médecins ou des biologistes et qui sont nécessaires dans le cadre de la médecine préventive, le diagnostic, etc.
    - Les traitements relatifs aux délits, aux condamnations ou aux mesures de sûreté
    - Les traitements relatifs aux interconnexions de fichiers aux finalités différentes

Protection des Données Personnelles

• Obligations applicables à la personne physique ou morale traitant les données

• Obligation de <u>sécurité</u>:

- La personne traitant les données doit mettre en oeuvre toutes les mesures techniques et organisationnelles appropriées pour protéger les données contre les risques suivants:
  - destruction accidentelle ou illicite des données,
  - perte accidentelle,
  - altération des données,
  - accès ou divulgation non autorisé,
  - et contre tout autre traitement illicite

- a fortiori lorsque les données sont transmises par le biais d'un réseau électronique.

Protection des Données Personnelles

• Obligations applicables à la personne physique ou morale traitant les données

- Obligation de sécurité:
  - Les mesures de sécurité doivent être décrites dans le formulaire de déclaration à la CNIL (art 34 de la loi Informatique et Liberté)

  - Les mesures de sécurité doivent être appliquées préalablement à la mise en oeuvre du traitement de données
    - Contrôles sur la fiabilité des équipements et des logiciels utilisés, avec possibilité d'un audit préalable pour tester des problèmes éventuels d'erreurs ou d'omissions, etc. pouvant donner des résultats incorrects avec des conséquences négatives sur les personnes concernées.
    - Evaluation générale de la sécurité et des risques

Protection des Données Personnelles

- **Obligations applicables à la personne physique ou morale traitant les données**

- Obligation de sécurité:
  - L'obligation de sécurité s'applique également à l'archivage des données
    - La CNIL a publié une décision concernant les procédures et les mesures de sécurité applicables à l'archivage des données à caractère personnel

- Enfin, l'obligation de sécurité est également applicable aux tiers traitant les données pour le compte d'une entreprise

- Tout manquement aux obligations de sécurité peut entraîner la mise en oeuvre de la responsabilité pénale: 5 ans d'emprisonnement et/ou 300.000€ d'amende (x5 lorsque la personne fautive est une personne morale)

Protection des Données Personnelles

- **Obligations applicables à la personne physique ou morale traitant les données**

- **Auto-régulation et Codes de conduite:**

  - Les organisations professionnelles et les associations peuvent développer leur propre système d'auto-régulation concernant la prospection et la collecte des données à caractère personnel.

  - Par exemple, les associations marketing suivantes ont développé des codes de conduite, approuvés par la CNIL les 22 et 30 mars 2005: le Syndicat national de la communication directe (SNCD) et l'Union française du marketing direct (UFMD).

Protection des Données Personnelles

- **Résumé de la protection des données personnelles au niveau européen : 6 principes fondamentaux**

- Notification: droit de la personne concernée à être informée sur les catégories d'informations collectées et sur la façon dont elles sont utilisées
- Accès: droit de la personne de savoir quelles données sont collectées et droit de correction, mise à jour, etc. des données
- Intégrité des données: obligation du responsable du traitement de s'assurer que les données sont correctes et à jour
- Sécurité: droit à ce que les données soient stockées dans un endroit sûr
- Choix: droit d'autoriser (ou refuser) les transferts de données a priori, et droit de s'opposer à l'utilisation des données en marketing direct
- Opposabilité: droit à une réparation appropriée en cas de violation de la loi

Protection des Données Personnelles

- **Règles spécifiques applicables à la protection des données et à l'internet**

- Sites web
- Cookies
- Sollicitation commerciale et Spamming
- Données de connexion

Protection des Données Personnelles

- **Règles spécifiques applicables à la protection des données et à l'internet**

- **Sites web**

  - Collecte des données: sur certains sites web, il peut être demandé de remplir un questionnaire (ex. sites de e-commerce). Ces questionnaires doivent préciser quelles questions/réponses sont obligatoires pour pouvoir fournir le service ou traiter la commande et lesquelles sont optionnelles.

  - Les fichiers de données personnelles collectées par l'intermédiaire du web sont soumis à toutes les dispositions de la loi Informatique et Libertés à partir du moment où le site vise le public français (en France) et/ou est exploité par une personne morale de droit français.

Protection des Données Personnelles

- **Règles spécifiques applicables à la protection des données et à l'internet**

- **Cookies**
  - **Les cookies sont des petits logiciels dont l'objet est de collecter des données à l'insu de l'internaute. Les données collectées permettent ensuite d'identifier le profil des utilisateurs: fréquence de retour sur le site, type et nombre de pages vues, etc.**
  - **Les cookies sont utilisés en premier lieu à des fins de marketing**

  - **L'utilisation des cookies par les sites web est autorisée, sous réserve d'obtenir le consentement des utilisateurs.**
  - **Toute absence de notification est constitutive d'un délit (art 226-18 du code pénal)**

Protection des Données Personnelles

- **Règles spécifiques applicables à la protection des données et à l'internet**

- **Données de connexion**

  - Jusqu'à récemment, la CNIL recommandait que les données de connexion ne soient conservées que pour la durée de la transmission des données (délibération de juillet 1997)

  - Un certain nombre d'exceptions ont par la suite été admises: les FAI et opérateurs de télécom ont été autorisés à conserver les données de connexion à des fins de facturation et de paiement; également aux fins d'aider les autorités de police et la sécurité nationale.

Protection des Données Personnelles

- **Règles spécifiques applicables à la protection des données et à l'internet**

- **Données de connexion**

  - La LCEN du 21 juin 2004 dispose que les FAI et les hébergeurs doivent conserver les données de connexion pendant une période d'un an et divulguer ces données aux autorités/forces de l'ordre à leur demande afin de les aider dans le cadre de leurs enquêtes

  - Finalement complété par le décret du 25 février 2011 "relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu en ligne"

Protection des Données Personnelles

- **Règles spécifiques applicables à la protection des données et à l'internet**

- **Sollicitation commerciale et Spamming**

  - Les traitements de données dans un but de prospection commerciale sont soumis aux dispositions de la loi Informatique et Libertés à partir du moment où le public concerné est situé en France

  - La personne concernée doit donner sont consentement libre, spécific et informé pour la collecte (système de l'opt-in), sauf concernant les messages marketing pour des produits ou services identiques ou similaires à ceux préalablement fournis (système de l'opt-out autorisé)

Protection des Données Personnelles

- **Exemple d'email de sollicitation commerciale légal**

From: contact@wkf.fr
Subject: **Offre de Noël Spécial Internet**
Date: December 4, 2008 3:32:15 PM CEST
To: benedicte.deleporte@wanadoo.fr
Reply-To: contact@wkf.fr

Si vous avez des difficultés pour visualiser ce message, cliquez ici

À vos marques… prêts ?

> Éditions Lamy
> Liaisons Sociales

Partez… pour 15% de remise* !

Fiscalité et Comptabilité
Droit Immatériel
Droit des Affaires
Droit civil - Droit Pénal - Procédure
Droits Spécialisés
Collectivités Publiques et Associations

* Offre valable jusqu'au 25/12/2008 sur nos offres d'abonnement, non cumulable avec d'autres offres et hors promotions en cours.

Wolters Kluwer France
1, rue Eugène et Armand Peugeot - 92856 Rueil-Malmaison cedex
Confidentialité des données : conformément à la Loi Informatique et Libertés du 6 Janvier 1978, vous disposez d'un droit d'accès et de rectification des données vous concernant. Vous recevez cette invitation car vous avez été en contact avec le Service Commercial de Wolters Kluwer France ou de ses partenaires. Pour ne plus recevoir de messages de Wolters Kluwer France cliquez ici.

Protection des Données Personnelles

- **Règles spécifiques applicables à la protection des données et à l'internet**

- **Sollicitation commerciale et Spamming**

- Le spamming est illégal ! Pour être considéré comme du "spamming", une campagne d'emailing doit remplir 3 conditions cumulatives:

- **1) consiste en l'envoi en masse d'emails**
- **2) non-sollicités à un grand nombre de destinataires**
- **3) avec lesquels l'émetteur n'a pas de contacts pré-existants.**

- Les adresses email ont généralement été collectées de manière illicite.

- La pratique du spamming est différente de la prospection commerciale/ sollicitation qui sont des pratiques licites

Protection des Données Personnelles

- **Exemple de spam**

From: zwasyhwamodu@presidentialclassroom.org
Subject: *** SPAM ***Un déjeuné gratuit ça vous dit ?
Date: January 13, 2009 11:28:18 AM CEST
To: lamagnanne@wanadoo.fr
Cc: gosse.marcel@wanadoo.fr, cyril.pledel@wanadoo.fr, lejeunee@wanadoo.fr, chyc.lafuteur@wanadoo.fr, lamanonegra@wanadoo.fr, anegba.manga@wanadoo.fr, axel.bergeron@wanadoo.fr, ludovic-chapon@wanadoo.frand 6 more…

Un déjeuné gratuit ça vous dit ?

Votre mère avait peut-être raison quand elle vous disait qu'il n'y a rien de mieux qu'un déjeuné gratuit. Elle savait de quoi elle parlait quand elle disait que l'argent ne pousse pas sur les arbres Mais elle n'aurait jamais pu deviner que vous pourriez gagner un bonus de 555 € sur Privilege Club Casino.

Déposez seulement 100 € et vous jouerez avec 400 € !
Ajoutez à nouveau 100 € et vous jouerez avec 200 € de plus
Déposez encore 100 € et nous vous offrirons 255 €

Alors allez-y, déjeunez. C'est nous qui offrons !

http://www.timegoldgaming.net/fr/

Protection des Données Personnelles

- **Exemple de spam**

From: "VerifiedByVisa"<Verified@Visa.fr> **Subject:** **[SPAM]VotreCarteBancaireestsuspendue!**
Date: October 30, 2011 2:44:33 PM GMT+01:00

Cher Client Carte Visa,

Il a été porté à notre attention que votre carte Visa informations doit être réactivée as part of our continuing commitment to protect your card and pour réduire l'instance de la fraude. Une fois que vous avez réactivé votre carte Visa documents, votre carte
service ne sera pas interrompu et continuera comme d'habitude. Votre numéro d'identification du cas est la suivante:**YSZ477DS582LT** Pour réactiver votre carte Visa cliquez sur le lien suivant: S'il vous plaît cliquez sur ici pour vérifier votre identité
Défaut de vérifier votre dossiers se traduira par carte Suspension
Service Carte de crédit.
International Sécurite

Protection des Données Personnelles

- Les transferts de données à l'international

  - Trois cas de figure peuvent se présenter

    - 1) Transfert de données à l'intérieur de l'Union européenne
    - 2) Transfert de données à l'extérieur de l'UE, vers un pays présentant un niveau de protection suffisant
    - 3) Transfert de données à l'extérieur de l'UE, vers un pays ne présentant pas un niveau de protection suffisant

Protection des Données Personnelles

- **Les transferts de données au sein de l'Union européenne**

- L'un des objectifs principaux de la Directive sur la protection des données de 1995 a été de créer un ensemble de règles relatives à la protection de la vie privée commun à tous les pays membres de l'UE:

- pour établir un système de protection de haut niveau équivalent dans tous les Etats-membres de l'UE et

- pour éliminer les obstacles aux échanges de données nécessaires au bon fonctionnement du marché intérieur.

- Nécessité d'équilibrer les finalités de libre circulation des données personnelles entre les Etats-membres tout en sauvegardant les droits fondamentaux des personnes

Protection des Données Personnelles

- **Les transferts de données au sein de l'Union européenne**

  - Principe: pas de restrictions aux transferts de données à caractère personnel vers un autre Etat-membre

    - ou vers un pays membre de l'EEE (Espace économique européen - Islande, Norvège, Liechtenstein)

Protection des Données Personnelles

- **Les transferts de données internationaux en dehors de l'UE - vers un pays présentant un niveau de protection suffisant**

  - Principe: tout transfert de données personnelles en dehors de l'UE est soumis à la condition que le pays destinataire fournisse un niveau suffisant de protection de la vie privée et des droits fondamentaux des personnes (Art 68 de la loi Informatique et Libertés) - à savoir un <u>niveau de protection adéquate</u>

    - La Commission Européenne est la seule autorité pouvant décider quels pays paraissent présenter un niveau adéquat de protection de la vie privée, compte tenu des critères figurant dans la Directive de 1995.
    - A ce jour, seul un nombre très limité de pays ont été admis comme présentant ce niveau de protection: l'Argentine, le Canada, Guernesey, l'Ile de Man, Israël, Nouvelle Zélande, la Suisse, l'Uruguay
      - Pour les Etats-Unis, seules les sociétés ayant choisi de se conformer aux principes du Safe Harbor sont concernées

Protection des Données Personnelles

- Les transferts de données internationaux en dehors de l'UE - vers un pays ne présentant pas un niveau de protection suffisant

  - Principe: aucun transfert de données personnelles vers un pays non-membre de l'UE ne présentant pas un niveau de protection adéquat n'est autorisé

    - Inclus les transferts de données intra-groupes, à savoir les transferts entre les sociétés d'une même groupe mais opérant dans des régions du monde différentes.

  - sauf si le destinataire s'engage à fournir un niveau de protection de la vie privée suffisant

Protection des Données Personnelles

- Les transferts de données internationaux en dehors de l'UE - vers un pays ne présentant pas un niveau de protection suffisant

  - Les sociétés peuvent cependant décider individuellement de se conformer aux obligations de fournir un niveau de protection suffisant aux données à caractère personnel transférées vers des pays qui n'offrent pas par ailleurs un niveau de protection adéquat.

- Trois systèmes ont été développés pour permettre aux entreprises de transférer des données à l'international
  - Le contrat standard de transfert de données (EU)
  - Les Safe Harbor Principles (Etats-Unis uniquement)
  - Les Binding Corporate Rules (BCRs)

Protection des Données Personnelles

- **Les transferts de données internationaux en dehors de l'UE - vers un pays ne présentant pas un niveau de protection suffisant**

  - Le <u>contrat standard de l'UE de transfert de données</u>

    - La Commission Européenne a développé un contrat standard de transfert de données (publié en 2001 et modifié en 2004). Ce document comprend un certain nombre d'obligations à la charge de l'importateur des données:

      - Mise en oeuvre de procédures de sécurité applicables au transfert de données et au traitement; Respect de la finalité du traitement de données; Identification d'un service interne responsable du suivi des demandes de l'exportateur des données et de la CNIL, ainsi que des questions posées par les personnes concernées. L'exportateur des données doit s'assurer que l'importateur est capable de respecter les obligations légales.

      - Les entreprises ne sont pas obligées d'utiliser le contrat standard. Si elles l'utilisent, aucune stipulation contractuelle ne peut être modifiée (principe du 'tout ou rien')

Protection des Données Personnelles

- Les transferts de données internationaux en dehors de l'UE - vers un pays ne présentant pas un niveau de protection suffisant

  - Les Safe Harbor Principles (ou "Sphère de sécurité")
    - Développé par le ministère du commerce américain (US Commerce Department) et reconnu par la Commission européenne comme présentant un niveau de protection adéquat. Accord date du 26/07/2002.

    - Les Etats-Unis privilégient le principe de l'auto-régulation et du contrat en matière de protection des données à caractère personnel

    - Le principe général reste l'interdiction des transferts de données personnelles vers les Etats-Unis
      - sauf vers les sociétés ayant volontairement et publiquement adhéré aux principes du Safe Harbor qui sont présumées offir un niveau de protection adéquat

Protection des Données Personnelles

- Les transferts de données internationaux en dehors de l'UE - vers un pays ne présentant pas un niveau de protection suffisant

  - Les Safe Harbor Principles (ou "Sphère de sécurité")
    - Des FAQs complètent le dispositif avec un rappel des règles de base, notamment:
      - Principe d'information préalable de la personne concernée
      - Faculté d'opposition
      - Obligation de recueillir l'accord exprès de la personne concernée pour la collecte de données sensibles
      - Engagement de prendre les mesures nécessaires pour assurer la sécurité du traitement et l'intégrité des données, etc.

- La liste des entreprises adhérentes au Safe Harbor est dressée par le Ministère du Commerce US et publiée dans un registre public

Protection des Données Personnelles

- Les transferts de données internationaux en dehors de l'UE - vers un pays ne présentant pas un niveau de protection suffisant

  - Toutes les entreprises américaines ne choisissent pas de se conformer aux principes de Safe Harbor

  - Dans le cadre des transferts internationaux de données à caractère personnelle, elles peuvent également choisir de mettre en place des systèmes de transfert régis contractuellement:

    - Contrat de protection de la vie privée
    - Binding corporate rules (BCRs)

Protection des Données Personnelles

- Les transferts de données internationaux en dehors de l'UE - vers un pays ne présentant pas un niveau de protection suffisant

  - Toutes les entreprises américaines ne choisissent pas de se conformer aux principes de Safe Harbor

  - Les <u>contrats de protection de la vie privée</u>:
    - 2 sociétés, l'une exportatrice de données située dans l'UE et l'autre, importatrice des données située en dehors de l'UE (aux US ou ailleurs) peuvent également développer leur propre contrat de protection de données personnelles et le soumettre à l'approbation de la CNIL

Protection des Données Personnelles

- Les transferts de données internationaux en dehors de l'UE - vers un pays ne présentant pas un niveau de protection suffisant

  - Toutes les entreprises américaines ne choisissent pas de se conformer aux principes de Safe Harbor

  - Les Binding Corporate Rules (BCRs - ou règles internes d'entreprise)

    - Système similaire à un contrat intra-groupe (ex. General Electric, Microsoft) contenant un ensemble de règles applicables à la protection des données personnelles et aux transferts de données à l'intérieur du groupe. Les BCRs sont communiquées à la commission de protection de la vie privée de l'un des pays de l'UE (la CNIL par ex) pour approbation/validation. Une fois approuvées par une commission au sein de l'UE, les BCRs de ce groupe seront automatiquement reconnues comme validées par les autres commissions.

    - Système développé par quelques grandes entreprises et validé au niveau européen par le "groupe de l'article 29" (groupe des représentants des commissions vie privée des différents Etats-membres)